ABSTRACT OF THE DISCLOSURE

A certificate management method is provided whereby a plurality of service providers have different reliable certificate authorities and, when certificates issued from the certificate authorities are implemented into a smart card, merely by revoking the certificate issued from the certificate authority on which the first service provider relies, all other implemented certificates can be revoked, and the certificates can be individually revoked. A system for implementing the method is provided. The certificate authorities n ($n \geq 2$) issue a certificate n by using a private key n' corresponding to certificate n' generated by using a certificate 1 issued from a certificate authority 1 which has previously been installed in the smart card and a corresponding private key 1. Thus, the issued certificates have a hierarchical chain relation. When the user wants to revoke all certificates, the certificate 1 issued from the certificate authority 1 is revoked.